15 STEPS TO CYBER SECURITY FOR BUSINESS

IT'S TIME TO LOCK THE DATA DOOR.

What gaps in your business' cyber security might leave you exposed to a breach?

1. MAINTAIN PASSWORDS

DO use a different password for every login
Make sure your passwords follow best practice
Store your passwords securely using a password manager
Consider single sign on.

DON'T use the same password across multiple sites or services. Store your passwords in your internet browser. Share passwords throughout your team.

2. PAYMENTS

DO make sure any money you send is going where you think it is.

3. ATTACHMENTS

DO check attachment validity by calling the sender if you're in any doubt.

DON'T open attachments from people of businesses you don't know.

4. TWO & MULTI-FACTOR AUTHENTICATION

DO use two-factor or multi-factor authentication whenever it's available.

5. LINKS

DO check link validity if you're in any doubt by calling the sender.

DON'T click on suspicious links in emails or on websites.

6. KEEP SOFTWARE UPDATED

DO update your software regularly.

DON'T run software that is no longer supported (end of life).

7. BACKUP & HAVE A DISASTER RECOVERY PLAN

DO have a monitored backup system in place. backup regularly and check your backup regularly. Make sure your business has a disaster recovery plan.

DON'T Neglect to backup.

8. USE A SECURE WI-FI CONNECTION

DO use a VPN to encrypt your data when connecting to public Wi-Fi. Use your mobile network instead of Wi-Fi when possible.

DON'T contact important business online while connected to public Wi-Fi unless you have a VPN connection..

9. SECURE YOUR MOBILE DEVICES

DO Ensure that your mobile phone uses password protection and fingerprint encryption. Minimise access to public Wi-Fi and switch off Bluetooth when possible. Have a company mobile phone policy.

DON'T leave your phone unattended in public places. Download files unless absolutely necessary.

10. SECURE YOUR PRINTERS

DO have a company printer policy in place to handle and manage documents. Don't leave printed documents unattended in the printer tray. Make sure you've set up and configured the printer settings correctly. Setup secure printer access via a password or security badges.

11. UNDERSTAND SOCIAL ENGINEERING

DO be aware of social engineering cyber attacks and have a policy for handling them. Train your staff. This is key in preventing social engineering attacks.

DON'T share information with anyone outside your company without making sure they're who they say they are.

12. NEVER LEAVE DEVICES UNATTENDED

DO encrypt all portable hard drives and USB devices. Physically lock unattended computers.

DON'T temporarily lock screens when not using your device.

13. POLICY

DO have a cyber security policy in place.

14. TRAINING

DO train your team regularly on best practice.

15. HAVE A RISK MANAGEMENT PLAN

DO have a risk management plan in place in case of a breach. Have reliable, experienced IT support.

DISCOVER AN EASIER WAY TO MANAGE YOUR I.T. YOU'LL BE GLAD YOU DID.

03 9874 5473
www.p1technology.com.au

P1 TECHNOLOGY